IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	Case No. 1:22-CR-183
v.	)	The Hon. Claude M. Hilton
MAX CHRISTIAN FREAR,	)	Bench Trial: January 17, 2023
Defendant.	)	

GOVERNMENT'S TRIAL BRIEF

On January 17, 2023, Max Christian Frear will appear for a bench trial on one count of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1), and one count of destruction or removal or property to prevent search or seizure, in violation of 18 U.S.C. § 2232(a). This Trial Brief provides an overview of how the United States will prove beyond a reasonable doubt that the defendant committed these acts and addresses evidentiary issues that may arise at trial.

FACTUAL BACKGROUND

From at least November 2019 through January 2022, the defendant used an Internet platform to search for and download child pornography[1] to his laptop hard drive. In February 2022, when the defendant realized that law enforcement was preparing to search his home, he attempted to destroy his collection of child pornography by flushing the hard drive down the toilet. Despite his attempt to destroy it, law enforcement recovered the hard drive from the toilet and

[1] The term "child pornography" will be used in this Trial Brief to refer to visual depictions of minors engaged in sexually explicit conduct, as those terms are defined in 18 U.S.C. § 2256.

forensically examined it, thereby locating 84 videos and more than 5,600 image files depicting child pornography.

During its case-in-chief, the government will present the testimony of three law enforcement witnesses who will establish the following facts.

In 2021, the Federal Bureau of Investigation ("FBI") learned that a computer with Internet Protocol ("IP") address 71.62.185.6 (the "Target IP") was seeking to download suspected child pornography files via an Internet-based peer-to-peer (P2P)[2] software program called Freenet.[3] Freenet allows users to anonymously share files, chat on message boards, and access websites within the network. Freenet users often install Frost, a Freenet client which, like Freenet, also operates via the Internet. Freenet must be installed to use Frost, which provides an easy-to-use messaging board for users to share information related to finding and downloading content, including where to download content and the required keys or passwords to access the files.

According to Comcast records, the Target IP was assigned to a residence located in Round Hill, Virginia, which is located within the Eastern District of Virginia. *See* GX602, 602A. The defendant's father was the listed subscriber. Further investigation revealed that the defendant lived with his father and mother at this address.

[2] A P2P network is a group of computers, connected to each other via the Internet, where each computer acts as both a server and a client, storing, sending, and receiving files within the network.
[3] As detailed in Dkt. 31, the government will introduce only brief background evidence regarding the Freenet and Frost platforms to aid in understanding the forensic evidence. In its case-in-chief, the United States will prove that the evidence gathered from the search of the defendant's residence and his digital devices shows that the defendant knowingly received child pornography. The defendant did not seek to challenge the basis of the search prior to trial. Thus, the defendant should not be permitted to introduce or elicit evidence regarding the initial, pre-search warrant investigation.

I. The Residential Search Warrant

In January 2022, FBI Special Agent (SA) Tonya Griffith obtained a federal search warrant for the defendant's residence. That warrant authorized the search of the residence for, among other things, digital media devices related to child pornography. Law enforcement executed the search warrant on February 3, 2022. Almost immediately after the entry team knocked and announced their presence, the defendant's parents appeared at the front door. Several minutes later, the defendant emerged from his third-floor bedroom and came to the front door as well.

The search team then secured the residence and entered the home. Detective Jeremiah Johnson, a Task Force Officer (TFO) with the Metropolitan Police Department, surveyed the third floor, including an occupied bedroom, which the defendant later told law enforcement was his bedroom. As Detective Johnson walked into the bedroom's adjoining bathroom, he spotted a small black storage device in the toilet bowl. *See* GX124. Detective Johnson's colleague put on a glove, reached into the toilet, and removed the storage device, which turned out to be an SSD.[4] The SSD was bent in half and covered in a gray substance. Detective Johnson removed the in-tact inner memory chip from the metal casing to dry it out. *See* GX155. Detective Johnson noticed drops of gray liquid on the floor around the toilet bowl and also in a trail leading from the bathroom to a 3D printer on a desk in the adjoining bedroom. *See* GX124, GX128, GX130. Detective Johnson informed the agents interviewing the defendant about the SSD recovered from the toilet bowl.

II. Interview of Defendant

While agents searched the defendant's house, FBI SA Derek Goguen, the primary case agent, and SA Laura Calvillo interviewed the defendant on the porch at his residence.[5] The

[4] An SSD functions in the same way as a hard drive, but it has a different operating mechanism.
[5] Loudoun County TFO Corinne Czekaj was also present for the interview.

interview was audio recorded and lasted approximately 1 hour and 45 minutes.[6] *See* GX104-107; GX301.

During the interview, the agents told the defendant that the SSD was recovered intact and was drying out. They asked the defendant what they would find on it. The defendant admitted they would find child pornography, which he defined as having "very young" children—"less than 13." GX301A, 302A. The defendant said those files came from Freenet and that he downloaded them over the course of years. *Id.* During the interview, the defendant explained how Freenet worked and why he used it (instead of, for instance, Tor). *See, e.g.,* GX301C, 302C. The defendant estimated there were 30 or 40 videos he downloaded from Freenet. He admitted that he would find videos he would watch more than one time. *See* GX301B, 302B. He also deleted content because "there's a lot that I don't like." *Id.* He was interested in content that was "weird enough." *See* GX301D, 302D. Terms such as "hand job", "5yo", "infant", and "toddler and babysitter" would pique his interest. The defendant also downloaded and watched Omegle child pornography reaction videos, which capture the reaction of people (often minors) who are confronted with child pornography on the Omegle video chat application. Notably, the defendant admitted that he saved all these child pornography files in the automatic Downloads folder; after receiving them onto his computer, he did not move them elsewhere on the computer, or create subfolders within the Downloads folder. Nor did he change any file names. He explained, "I just leave it there."

The defendant also admitted that he tried to destroy the SSD to prevent law enforcement from searching it. *See* GX301E, 302E. The defendant stated that once he realized it was law enforcement, he thought they were here because of the child pornography. So, he grabbed his

[6] At this point, the government has no reason to believe that the defendant is challenging the voluntariness of his interview. Regardless, evidence supporting its voluntary nature will be elicited at trial.

ASUS laptop out of his backpack. He pulled the SSD out of the laptop, dunked it in resin, tried to break it, and then flushed it down the toilet. He was "pretty sure" he broke it and "didn't notice" that the SSD did not actually flush. Then he came downstairs. As the defendant admitted, the SSD was the only device to contain child pornography; in his words, "Nothing should have escaped that hard drive."

During the interview, the defendant provided relevant background information, including his birth date, cell phone number, email addresses, and online gaming usernames. He said he last left the residence in the summer 2021 for a vacation, where he had no Internet access. The defendant said he runs his own media preservation business and works at Home Depot in Leesburg, within the Eastern District of Virginia.

III. Forensic Examination of the SSD

At the conclusion of the search, approximately 13 electronic devices, including the SSD and ASUS laptop, were seized, tagged, and entered into evidence. Pursuant to the search warrant, the FBI then forensically examined the seized electronic devices. Those examinations corroborated the defendant's statements. Of the devices seized, only the SSD contained child pornography. Moreover, the laptop's SSD slot was empty.

SA Griffith, who is a certified digital extraction technician (DEXT), made a forensic copy of the SSD using a TX1 forensic imager. SA Griffith will testify that the TX1 has certain built-in accuracy checks and quality assurance mechanisms, including a write blocker[7] and hash

[7] SA Griffith will testify that based on her training and experience, a write blocker is a tool designed to prevent any modification of the data contained within a device that is being copied to another drive. *See* Dkt. No. 33 (Expert Notice).

verification.[8] She then processed the forensic copy using Axiom, a forensic program, and uploaded the processed, readable data to the FBI server for the case agent to review.

SA Goguen reviewed the contents of the SSD using forensic programs Axiom and Griffeye. SA Goguen found evidence of the defendant's extensive use of the Internet-based platforms Frost and Freenet, which had been downloaded to the SSD before November 2019. *See* GX 506. At the time of seizure, the SSD contained 84 child pornography videos in the following folder: C:\Users\Trashman\Downloads\frost 2011 03-05\frost\downloads. *See* GX508. SA Goguen will testify that this folder is the default folder location for files downloaded from Frost. All of the videos in this folder contained child pornography. And many of the videos depict the violent sexual abuse of infants and toddlers; some of them last for longer than 30 minutes. In total, that folder contained 810 minutes of content. *See* GX507. These videos were created in the folder (*i.e.*, downloaded) between February 21, 2020 and December 3, 2021. The SSD also contained 5672 images depicting child pornography in a folder associated with web browsing. *See id.*

[8] A hash is a unique alphanumeric string that serves "essentially [as] a fingerprint of a digital file." *United States v. Willard*, 2010 WL 3784944, at *1 n.1 (E.D. Va. Sept. 20, 2010) (Spencer, J.). By comparing the hash value of two files, "investigators can determine whether the files are identical with precision greater than 99.9999 percent certainty." *Id.* Since the likelihood of two different pieces of electronic evidence randomly having the same hash value is extremely remote (2^160 for SHA-1), federal courts have relied on hash values to admit evidence at trial. *See, e.g.*, *United States v. Glassgow*, 682 F.3d 1107 (8th Cir. 2012). Thus, the government may properly offer exhibits of data that was stored on the defendant's SSD, even though the data was not taken directly from the SSD.

SA Goguen reviewed all the child pornography media on the SSD and will testify that the image and video files he reviewed depict minors engaged in sexually explicit conduct.[9] At trial, SA Goguen will testify about six videos in particular that he found in the Frost Downloads folder. *See* Dkt. 30. All of them were recently played in VLC Media Player.[10] They constitute a representative sample of the child pornography files the defendant knowingly received via the Internet and accessed on his SSD:

- "Dad w/3yo daughter"—This approximately 3-minute, 36-second video depicts a nude adult male bathing with a nude female toddler in between his legs. The minor victim masturbates and licks the adult male's erect penis while in the tub. The video then cuts to a separate scene where a nude female toddler is laying on her back on top of a black towel and a nude adult male attempts to insert his erect penis into the vagina of the minor victim, before he masturbates and ejaculates on the minor victim's bare vagina and stomach. *See* GX402, 402A.
- "5yo sucking" – This approximately 5-minute, 15-second video depicts a minor male victim performing oral sex on an adult male. *See* GX403, 403A.
- "Josephine #1 natural born cock lover" – This approximately 3-minute, 24-second video depicts an adult male penetrating a nude infant female's vagina with his fingers. The video then cuts to a separate scene where a nude adult male inserts his erect penis into the mouth of a nude infant female before he masturbates and ejaculates in the mouth and on the face of the minor victim. *See* GX404, 404A.
- "Josephine #2 let me play with your dick and I let you play with my cucumber" – This approximately 1-minute, 34-second video depicts a nude female infant with a pacifier masturbating an erect penis. An adult male then uses the pacifier to digitally penetrate the infant. *See* GX405, 405A.

[9] Notwithstanding any related evidence the government may introduce at trial, the Court is capable of determining on its own that the proffered images of child pornography depict real victims under the age of 18. "[T]here seems to be general agreement among the circuits that pornographic images themselves are sufficient to prove the depiction of actual minors." *United States v. Bynum*, 604 F.3d 161, 166 (4th Cir. 2010) (quoting *United States v. Salcido*, 506 F.3d 729, 734 (9th Cir.2007) (per curiam) (collecting cases)). The factfinder, in other words, can determine for itself whether a child is real and under the age of 18. Not requiring the government to call a witness to establish this fact is particularly appropriate where, as here, the videos unambiguously depict children under the age of 18.

[10] VLC Media Player automatically keeps track of the 30 most recently played video files. The media player also captures the file path of the video and how long a user viewed the video before pausing or stopping.

- "Josephine #5 dick addicted" – This approximately 3-minute, 17-second video depicts a nude female infant whose anus and vagina are lasciviously spread apart by an adult male. The adult male then digitally penetrates the infant's vagina before placing his erect penis in her mouth and ejaculating. *See* GX406, 406A.
- "OMEGLE_Vol.10.mkv" – This approximately 33-minute video depicts a compilation of numerous videos of minors engaging in sexually explicit conduct, including vaginal penetration and oral sex. These videos are played on the chat application "Omegle" and also capture the reaction of unsuspecting minors who are confronted with this material. *See* GX407, 407A.

For each of these videos, the government has prepared a storyboard, which is a series of still images from the video that is automatically generated by a computer program. *See* GX402B, 403B, 404B, 405B, 406B, 407B.

SA Goguen will testify that forensic examination of the SSD uncovered numerous forensic artifacts which show the defendant was downloading and viewing child pornography since as early as November 22, 2019. These artifacts include LNK files,[11] Jump List entries,[12] and VLC recently played information. *See* GX510, 510A, 511, 511A, 512. The government has prepared summary charts for each video file in GX402-407, which shows related forensic artifacts found on the SSD for each video. *See* GX402B, 403B, 404B, 405B, 406B, 407B. For instance, the Josephine #2 video was created in the Frost Downloads folder on June 5, 2021. The video was accessed as recently as January 30, 2022, just days before the search warrant. *See* GX405B. In addition, although the SSD contained 3 videos in the "Josephine" series (Josephine #1, #2, and #5), Jump List entries indicate that the defendant had also accessed "Josephine #3 Gentle touching" and "Josephine #4 Train my throat," both of which had been created in the Frost Downloads folder on

[11] A LNK file is automatically created by the operating system whenever a user opens a file. The computer retains that information even after the file itself is deleted.

[12] The Jump List is a shortcut file that allows the computer to remember where files are stored and which program is used to open them. One way a Jump List entry is created is when a user views a file using a program on the computer. The Jump List entry then records where the file was and what program was used to view it.

June 5, 2021. *See* GX511A. These two video files were not on the device at the time of seizure. This evidence is consistent with the defendant's own description of his child pornography collecting practices—he kept the videos he liked and deleted those he did not.

APPLICABLE LAW

The Indictment charges: (1) from on or about November 21, 2019 through on or about January 30, 2022, the defendant knowingly received and attempted to receive one or more visual depictions of minors engaged in sexually explicit conduct via the Internet; and (2) the defendant knowingly attempted to destroy property—namely, the SSD—for the purpose of preventing and impairing the government's lawful authority to take said property into its custody and control. *See* Indictment, Dkt. 1.[13]

I. Count One: Receipt of Child Pornography

To sustain its burden of proof for the crime of receipt of child pornography, the United States must prove the following essential elements beyond a reasonable doubt:

(1) The defendant knowingly received, or attempted to receive any visual depiction;

(2) The defendant did so using any means or facility of interstate or foreign commerce;

(3) The producing of the visual depiction involved the use of a minor engaged in sexually explicit conduct,

(4) The visual depiction is of a minor engaged in sexually explicit conduct; and

(5) The defendant knew that the visual depiction involved the use of a minor engaging in sexually explicit conduct.

[13] Venue is proper in the Eastern District of Virginia on both counts. At trial, the government will prove that the defendant engaged in the charged conduct from his home in Round Hill, Virginia, within the Eastern District of Virginia.

See 18 U.S.C. § 2252(a)(2); *see also United States v. Cedelle*, 89 F.3d 181, 185 (4th Cir. 1996).

While the relevant statute does not define what it means to *knowingly receive* child pornography, courts generally adopt "the common-sense understanding of the term." *United States v. Osborne*, 935 F.2d 32, 34 n.2 (4th Cir. 1991); *see also United States v. Ramos*, 685 F.3d 120, 131 (2d Cir. 2012) ("The statute does not define receipt or possession, and courts have given these terms their plain meaning."). The "ordinary meaning of 'receive' is 'to knowingly accept'; 'to take possession or delivery of'; or 'to take in through the mind or sense.'" *United States v. Pruitt*, 638 F.3d 763, 766 (11th Cir. 2011) (quoting *Webster's Third New International Dictionary: Unabridged* 1894 (1993)). To be sure, there is "no . . . question" that a defendant knowingly received child pornography "where [he] actively used a computer to solicit obscene material through numerous and repetitive searches and ultimately succeeded in obtaining the materials he sought." *United States v. Whorley*, 550 F.3d 326, 334 (4th Cir. 2008).

In addition to proving his knowing receipt of the child pornography, the government must prove the defendant's "knowledge of 'the sexually explicit nature of the materials as well as . . . the involvement of minors in the materials' production . . . ." *United States v. Miltier*, 882 F.3d 81, 86 (4th Cir. 2018) (quoting *United States v. Matthews*, 209 F.3d 338, 351 (4th Cir. 2000)). To satisfy this element "a defendant simply must be aware of the general nature and character of the material and need not know that the portrayals are illegal." *United States v. Knox*, 32 F.3d 733, 754 (3d Cir. 1994); *see also United States v. Wellman*, 663 F.3d 224, 230–31 (4th Cir. 2011) (recognizing that, under § 2252, "a defendant's knowledge of the law is not a relevant consideration"). The government can establish the defendant's knowledge of the nature and character of the material through circumstantial evidence, such as the presence and amount of child pornography files on a defendant's computer, the titles of the files of child pornography, the

defendant's ability to access the child pornography, and the frequency with which the defendant engaged in this activity. *United States v. Myers*, 560 F. App'x 184, 186–87 (4th Cir. 2014); *United States v. Freeman*, 1:14-CR-322 (JCC), 2015 WL 45521, at *8–10 (E.D. Va. Jan. 2, 2015).

At trial, the government will prove the defendant knowingly received child pornography via the Internet and stored the child pornography on his SSD. During his interview with law enforcement, the defendant admitted he used Freenet to download child pornography for years. When the agent asked him if he was looking for an age range, "like 5 YO, or infant, or toddler and babysitter, something like that?" the defendant replied "Sure. Those would pique my interest, something weird enough, I'd probably go for those." When the agents told the defendant that his SSD had been recovered from the toilet and they would be able to examine it, the defendant admitted that they would find child pornography on it. *See* GX302A.

The evidence will show that the defendant's SSD contained 84 video files and more than 5,600 image files depicting child pornography. The 84 video files were all saved in a Frost downloads folder, which is the default location for a file downloaded from Frost. The forensic examination of the SSD uncovered countless forensic artifacts which show that the defendant downloaded and accessed files with titles indicative of child pornography since as early as November 22, 2019 and as recently as January 30, 2022. Moreover, the defendant had 3 child pornography videos depicting the sexual abuse of the same female infant; he downloaded Josephine #2, Josephine #3, and Josephine #4 on June 5, 2021, and 10 days later he downloaded Josephine #1 and Josephine #5. These facts, taken together, leave no question that the defendant knowingly received visual depictions of a minor engaged in sexually explicit conduct.

Section 2252(a)(2) further requires that the defendant commit the crime using a "facility or means of interstate . . . commerce[.]" It is well established that the transmission of images or

video content by means of the Internet constitutes the use of a facility of interstate commerce. *See Miltier*, 882 F.3d at 87–88. Here, the government can prove through direct and circumstantial evidence that the defendant used the Internet to receive the visual depiction of a minor engaged in sexually explicit conduct. The defendant told law enforcement that he used the Internet—specifically, the Freenet platform—to download child pornography. The forensic evidence corroborates that admission; the SSD is replete with evidence that the defendant used Internet-based platforms Freenet and Frost to search for and download child pornography files. Accordingly, this element is satisfied for Count One.

II. Count Two: Destruction or Removal of Property to Prevent Search or Seizure

To sustain its burden of proof for the crime of destruction of property to prevent search or seizure, the United States must prove the following essential elements beyond a reasonable doubt:

(1) The defendant knowingly destroyed, damaged, wasted, disposed of, or took some other action toward property, or attempted to do so;

(2) This occurred before, during, or after a search or seizure of the property;

(3) The search or seizure was by a person authorized to make the search or seizure; and

(4) The action was done with the purpose of preventing or impairing the Government's lawful authority to take said property into its custody or control, or to continue holding said property under its lawful custody and control.

See 18 U.S.C. § 2232(a); *see United States v. Plavcak*, 411 F.3d 655, 660 (6th Cir. 2005); *see also United States v. Lessner*, 498 F.3d 185, 198 (3d Cir. 2007); *Gasho v. United States*, 39 F.3d 1420, 1430 (9th Cir. 1994).

The evidence will show that the defendant attempted to destroy his SSD to prevent its lawful search and seizure by law enforcement. To convict the defendant of attempted destruction

of property, the government must prove beyond a reasonable doubt that "(1) he had culpable intent to commit the crime and (2) he took a substantial step towards completion of the crime that strongly corroborates that intent." *United States v. Engle*, 676 F.3d 405, 420 (4th Cir. 2012). A defendant takes a substantial step when he "puts in motion events that would, from the defendant's point of view, result in the commission of a crime but for some intervening circumstance." *United States v. Pratt,* 351 F.3d 131, 135 (4th Cir. 2003). A "substantial act toward the commission of a crime need not be the last possible act before its commission." *Id.* Rather, "[a]n attempt comprises any substantial act in a progression of conduct that is meant to culminate in the commission of the crime intended." *Id.*

The evidence will show that in January 2022, a federal magistrate judge authorized a warrant to search the defendant's residence. That search warrant was based on information that someone at the defendant's home was downloading child pornography from Freenet. The search warrant authorized agents to search the home and seize electronic devices and evidence related to the investigation.

On February 3, 2022, law enforcement executed the search warrant at the defendant's residence. SA Goguen will testify that there was a noticeable delay between when the FBI knocked and announced at the front door and when the defendant presented himself. During the interview, the defendant admitted that once he realized law enforcement was there, he thought it was because of his child pornography. *See* GX302E. The defendant confessed he "was trying to figure out what [he] could do with [the device]. So I just put it in the toilet." *Id*. The defendant walked the agents through the steps he took to destroy his SSD: he grabbed his ASUS laptop out of his backpack, pulled the SSD out of the laptop, dumped the SSD in printer resin, then bent it in half and flushed

it down the toilet. *Id*. The defendant told the agents he was "pretty sure" he broke the device. *Id*. And when he went downstairs to meet them, he thought he flushed it. *Id*.

Detective Johnson will testify that he found the defendant's SSD bent in half, at the bottom of the toilet bowl; the government will seek to admit corresponding, illustrative photographs. The government will also seek to admit into evidence the obviously damaged metal casing of the SSD.

The evidence detailed above establishes that the defendant attempted to destroy the SSD for the specific purpose of preventing law enforcement's seizure of the device—the device that contained all the contraband evidence of child pornography. The defendant sought to prevent the government from taking control or possession of the SSD, and he only came downstairs after he thought he had successfully disposed of it. The United States submits that these proffered facts, taken together, leave no question that on February 3, 2022, the defendant intended to commit the crime of destruction of property to prevent search or seizure and that he took several substantial steps towards the completion of that offense.

EVIDENTIARY ISSUES

The parties have not entered into any stipulations at this time. The government anticipates that a number of legal issues may arise at trial. Although several of these issues are addressed below, the government reserves the right to supplement its position at trial.

I. Possession of Child Pornography is Not a Lesser-Included Offense in this Case

In this case, possession of child pornography, 18 U.S.C. § 2252(a)(4)(B), is not a lesser-included offense of receipt of child pornography. In the context of a jury trial, "a defendant is entitled to an instruction on a lesser included offense if the evidence would permit a jury rationally to find him guilty of the lesser offense and acquit him of the greater." *Keeble v. United States*, 412 U.S. 205, 208 (1973). However, a defendant "is not entitled to a lesser-included

offense instruction as a matter of course." *United States v. Smith*, 21 F.4th 122, 133 (4th Cir. 2021) (quoting *United States v. Wright*, 131 F.3d 1111, 1112 (4th Cir. 1997)). Instead, the district court "should ask whether 'proof on the element that differentiates the two offenses' is 'sufficiently in dispute' to necessitate instructing the jury on the lesser offense." *Id.* (quoting *United States v. Baker*, 985 F.2d 1248, 1258–59 (4th Cir. 1993)). "Such proof may be 'sufficiently in dispute' when there is evidence of 'sharply conflicting testimony' on that element or, in the absence of express conflict, when 'the conclusion as to the lesser offense fairly may be inferred from the evidence presented.'" *Id.* (quoting *Baker*, 985 F.2d at 1259). In making this assessment, "the district court must consider the totality of the circumstances." *Id.*

Although this is not a jury trial, the same principles hold: the element of "receipt" is not sufficiently in dispute to warrant a conviction of possession rather than receipt. *See, e.g.*, *United States v. Vallejos*, 742 F.3d 902, 906 (9th Cir. 2014) (holding that the district court "properly denied" the defendant's request for a lesser-included instruction on possession of child pornography where "[t]here was clear and undisputed evidence that [the defendant] knew he was downloading child pornography," such that "no rational jury could have found [him] guilty of possession but acquitted him of receipt"); *see also United States v. Hester*, 674 F. App'x 31, 34 (2d Cir. 2016) (holding that the district court did not plainly err by failing to give a lesser-included instruction on possession where the government "presented evidence that included: (1) nearly 100 emails from [his] email account in which he sent and received child pornography; (2) files from [his] Dropbox account where he shared child pornography with others; and (3) [the defendant's] confession admitting to sending and receiving child pornography"). Thus, the defendant should be convicted of receipt of child pornography and not simply possession.

II. The Government's Summary Exhibits Are Admissible under Federal Rule of Evidence 1006 and/or Rule 611(a)

The government has made available to the defense the computer forensic evidence in this case. This evidence, however, contains vast amounts of information processed by forensic tools; such information is voluminous and potentially confusing to persons lacking a background in technology. The only effective way to find and understand this evidence is to isolate excerpts. Yet, the import of the excerpts only becomes clear upon considering the various excerpts side-by-side. Consequently, during trial, the government will introduce summary charts under Federal Rule of Evidence 1006 that accurately reflect results from the forensic review of the SSD in this case. Specifically, the government intends to introduce at trial 7 summary exhibits, all of which have previously been provided to defense counsel. There are 6 summary exhibits related to the 6 child pornography exhibits the government intends to admit into evidence. These summary exhibits show the location of the video file on the SSD and relevant forensic artifacts. *See* GX402B, 403B, 404B, 405B, 406B, 407B. The location information and forensic artifacts are found within more voluminous computer forensic exhibits. The seventh summary exhibit is a timeline which shows when Freenet and Frost were downloaded to the SSD. *See* GX506. The information included in this exhibit is drawn from more voluminous computer forensic records.

The government asks that these charts be admitted into evidence under Rule 1006 because they contain summaries of the forensic examinations of the seized SSD that otherwise, based on the forensic results, are "voluminous writings . . . that cannot be conveniently examined in court." Fed. R. Evid. 1006. The government submits that the summary charts it intends to introduce at trial will accurately summarize authenticated evidence and assist the Court in understanding the complex computer forensics at issue in this case. *See United States v. Simmons*, 11 F.4th 239, 262

(4th Cir.), *cert. denied sub nom. Lassiter v. United States*, 142 S. Ct. 574 (2021); *United States v. Janati*, 374 F.3d 263, 272 (4th Cir. 2004).

The government also intends to introduce two sets of computer-generated screenshots. *See* GX701 and 702. These screenshots depict the steps necessary to download Freenet and Frost, including the default folder for downloaded content. This evidence is admissible under Federal Rule of Evidence 611(a). Under Rule 611, this court has "reasonable control over the mode and order of examining witnesses and presenting evidence so as to: (1) make those procedures effective for determining the truth; [and] (2) avoid wasting time; . . ." The decision whether to admit such summary evidence pursuant to Rule 611(a) is left to the sound discretion of the district court. *United States v. Johnson*, 54 F.3d 1150, 1158 (4th Cir. 1995). The Fourth Circuit has established guiding principles for a district court to consider when making that determination. A court must consider "whether the summary chart aids the jury in ascertaining the truth" and compare that to "the possible prejudice that would result to the defendant by allowing the summary chart into evidence." *See id.* at 1159. To minimize possible prejudice, courts should ensure that "the individual who prepared the chart—as well as the evidence upon which the preparer relied—was available for cross-examination by the defendant to test the competence of the evidence as presented in the summary chart." *Id.* Moreover, the jury should be instructed regarding "the manner in which they are to consider the charts." *Id.*

Government's exhibits 701 and 702 are admissible under Rule 611(a). They are clearly relevant: They show that C:\Users\Trashman\Downloads\frost 2011 03-05\frost\downloads is the default downloads folder for the Frost program and that C:\Users\Trashman\AppData\Local\Freenet\downloads is the default downloads folder for the Freenet program. This, in turn, shows that the child pornography files contained within either

folder were downloaded onto the device via the Internet. Although SA Goguen will provide oral testimony to this effect, the exhibits make this point in an understandable way. The visual depictions of the Freenet and Frost download process will assist the factfinder's understanding of the evidence, thus aiding the factfinder in ascertaining the truth. Moreover, any prejudice to the defendant will be minimal. The defendant has been provided these exhibits. He will have an opportunity to cross-examine SA Goguen and how he prepared these exhibits. Any prejudice is lessened in a bench trial. Here, there is no concern that the jury will rely on GX701 and GX702 without taking a closer look at the evidence upon which that chart is based. *See id.* at 1159.

Moreover, this evidence does not pose any hearsay problems. Courts consistently have held that machine-generated information is not hearsay as no "person" is making a statement. *See, e.g.*, *United States v. Washington*, 498 F.3d 225, 231 (4th Cir. 2007) (finding that machine-generated data used to determine whether a blood sample contained drugs or alcohol neither implicated the rule against hearsay nor the Confrontation Clause); *United States v. Hamilton*, 413 F.3d 1138, 1142-43 (10th Cir. 2005) (computer-generated "header" information, including the screen name, subject of the posting, the date the images were posted, and the individual's IP address, was not hearsay because no "person" acting as a declarant); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) (information automatically generated by fax machine is not hearsay because "nothing 'said' by a machine . . . is hearsay"). Thus, this evidence is properly admissible.

CONCLUSION

Based on the applicable law and the facts established by the evidence, the United States will ask this Court to find the defendant guilty of receiving and attempting to receive child pornography and destroying and attempting to destroy property to prevent search or seizure as

charged in the Indictment. Because this brief addresses only those factual and legal issues that the government currently foresees arising at trial, the government asks that the Court grant it leave to submit additional memoranda should other issues emerge later.

Respectfully submitted,

Jessica D. Aber
United States Attorney

Date: January 16, 2023

By: /s/

Lauren Halper
Assistant United States Attorney
Rachel L. Rothberg
Special Assistant United States Attorney (LT)
United States Attorney's Office
2100 Jamieson Ave.
Alexandria, Virginia 22314-5794
Phone: 703-299-3700
Fax: 703-299-3981
Email: Rachel.Rothberg2@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on January 16, 2023, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which automatically generated a Notice of Electronic Filing (NEF) and caused the NEF to be served electronically upon all counsel of record.

By: /s/

Rachel L. Rothberg
Special Assistant U.S. Attorney (LT)
U.S. Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Tel: 703-299-3700
Fax: 703-299-3981
Email: Rachel.Rothberg2@usdoj.gov